



REPLY TO  
ATTENTION OF

DEPARTMENT OF THE ARMY  
HEADQUARTERS, III CORPS AND FORT HOOD  
1001 761ST TANK BATTALION AVENUE  
FORT HOOD, TEXAS 76544-5000

**COMMAND POLICY  
PROT-01**

AFZF-PROT

JUL 24 2014

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Operations Security (OPSEC)

1. **APPLICABILITY.** This policy applies to all III Corps service members, Department of Defense Civilians, and all contracted or other personnel otherwise assigned to and under the operational control of III Corps.

2. **STATEMENT OF PURPOSE AND NECESSITY.**

a. Combat capability increasingly depends on gaining and maintaining information superiority. All aspects of raising, equipping, training, deploying, employing, and sustaining forces affect this superiority. Failure to protect information can result in serious injury or death to our personnel, damage to weapons systems, equipment and facilities, loss of sensitive technologies and mission failure.

b. Critical Information (CI) are facts and sensitive information about capabilities, activities, limitations, vulnerabilities, and intentions that help adversaries to plan against us, or interfere with our mission accomplishment (III Corps CI is enclosed). OPSEC protects CI from adversary observation and collection by identifying CI and indicators that might reveal it, and then developing measures to eliminate, reduce, or conceal those indicators.

c. Because of the potentially dire consequences of CI disclosure, OPSEC is everyone's responsibility. OPSEC applies at all times to all Army activities and all personnel associated therewith. It is required during training, sustaining, mobilizing, preparing for, and conducting operations, exercises, tests, or activities.

3. **POLICY.** This policy, AR 530-1, and the III Corps OPSEC Program require commanders at all levels to ensure their units or organizations integrate and implement OPSEC measures to protect CI. Every Army organization possesses information that ultimately affects the ability of U.S. forces to accomplish missions. Every organization must identify and protect information that an adversary could use against U.S. or other friendly forces. Every unit for which the commander or director is a lieutenant colonel or civilian equivalent or higher will establish and maintain a documented OPSEC Program that supports the III Corps and Fort Hood OPSEC Program and appoint in writing a Level

AFZF-PROT

SUBJECT: Operations Security (OPSEC)

II trained primary and alternate OPSEC Officer. All III Corps service members, Department of Defense Civilians, and all contracted or other personnel otherwise assigned to and under the operational control of III Corps will:

- a. Know what their organization considers to be CI, where it is located, who is responsible for it, how to protect it, and why it needs to be protected.
- b. Protect from disclosure any CI to which they have personal access to include CI from other branches of service, foreign governments, and contractor proprietary information.
- c. Not take pictures of military assets or share photographs displaying CI.
- d. Not publicly reference, discuss, share, or confirm CI that has already been compromised as this provides further unnecessary exposure of the compromised information and may serve to validate it.
- e. Actively encourage others, including family members and Family Readiness Groups (FRGs), to protect CI.
- f. Encrypt all emails that include sensitive information or CI on the unclassified network.
- g. Comply with command policy/direction as well as existing regulations prior to publishing or posting sensitive information that may be released into the public domain.
- h. Report attempts by unauthorized personnel to solicit CI per AR 381-12.
- i. Burn or shred CI that is no longer needed per the standards in AR 380-5 and AR 25-400-2, in order to prevent the inadvertent disclosure and reconstruction of this material.
- j. Remove access badges before leaving the building where the badge is required.

4. PUNITIVE ORDER. This policy is punitive and is intended to be a lawful general order and regulation within the meaning of Article 92, UCMJ, and 18 USC 1382. Violations of this policy may result in punitive action under the UCMJ, adverse administrative action, or both. Personnel not subject to the UCMJ who fail to protect sensitive and/or critical information from unauthorized disclosure may be subject to administrative, disciplinary, contractual, or criminal action.

AFZF-PROT  
SUBJECT: Operations Security (OPSEC)

5. EXPIRATION. This III Corps Command Policy Memorandum will remain in effect until superseded or rescinded.



KENDALL P. COX  
Major General, USA  
Deputy Commanding General

DISTRIBUTION:  
IAW FW FORM 1853: A

### III Corps Critical Information

1. Critical information (CI) consists of specific facts about our capabilities, activities, limitations, and intentions. CI is so vital to our mission that if the adversary obtains it, correctly analyzes it, and acts upon it, the compromise could prevent or seriously degrade mission success.

2. This critical information list (CIL) documents III Corps information that must be protected. III Corps CIL is as follows:

a. **Sensitive Reports**: reports containing sensitive and / or personally identifiable information (PII) or information pertaining to mission readiness such as blotters, battle damage assessments, recall rosters, manning documents, etc.

b. **Emerging TTP**: newly administered TTPs to improve mission effectiveness such as ways to avoid or detect IEDs, convoy protection methods, etc.

c. **Network and Communications Related**: call signs, frequencies, passwords, Automated Information Systems (AIS) protection (types used, measures, and procedures), changes in message volume, etc.

d. **Security Plans and Procedures**: Random Antiterrorism Measures, shift change for guards, changes in Force Protection Condition (FPCON), Defense Readiness Condition (DEFCON), or Information Condition (INFOCON), etc.

e. **Intelligence, Surveillance, and Reconnaissance (ISR)**: intelligence resources, collection techniques, ongoing operations and goals, counterintelligence operations, etc.

f. **Troop Movements and Travel**: deployment/redeployment Date Time Group (DTG), locations, itineraries, ports, routes, embarkation points, Very Important Person (VIP)/High Risk Personnel (HRP) travel, TDY orders, leave for large groups or entire units, emergency recall of personnel, etc.

g. **Information Pertaining to Current/Future Operations Planning**: deployment plans, exercises, scope of operations, planning details, specific COA for forces, ROE, Rules for the Use of Force, MISO and MILDEC operations, SAP elements in contracts, etc.

h. **Vulnerabilities**: any condition that allows the adversary time to observe, orient, Decide, and act against us in areas such as critical infrastructure, building schematics that show security weaknesses, physical security shortfalls, etc.

i. **Equipment Specifications and Limitations**: shortfalls, vehicle schematics, vehicle battle damage assessments, weapons systems, Research and Development (R&D) projects, electronic systems, software used in new systems, etc.

Encl